

Содержание

Настройка управления DPI. Интеграция через метод PUSH	3
<i>Удаленный запуск команд через SSH</i>	3
<i>Удаленный запуск утилиты fdpi_ctrl</i>	4

Настройка управления DPI. Интеграция через метод PUSH

Управление абонентами (Subscriber Management, SM) позволяет подключать услуги, управлять ограничением полосы (полисингом) и применять другие действия по отношению к отдельным абонентам. SKAT DPI идентифицирует абонентов по IP адресу, так как другой информации в IP пакете не присутствует, поэтому если выдача IP адресов абонентам производится динамически, необходимо произвести интеграцию с узлом выдачи адресов (RADIUS, DHCP) или установить компонент [FastRADIUS \(Монитор событий RADIUS. RADIUS Mapping\)](#).

Интеграция DPI платформы с биллингом по схеме PUSH подразумевает, что биллинг (или доп. система) должен самостоятельно сообщить на DPI информацию о подключенных абоненту услугах и настройках полисинга до их фактического применения на DPI. Переданные данные запоминаются во встроенной БД UDR и сразу активны после перезагрузки системы.



Рекомендуется использовать метод интеграции PULL (по протоколу RADIUS).
Продукт [BRAS](#).

Чтобы при перезапуске платформы восстановились настройки абонентских профилей, необходимо [активировать встроенную БД](#) или разместить скрипты инициализации в каталоге /etc/dpi/init.d/ (аналогично тому, как это обычно делается в linux при управлении шейпером или процессом загрузки). Последний вариант имеет свои преимущества и может оказаться подходящим решением для быстрой миграции с Linux/FreeBSD или аппаратных шейперов без собственной БД.

Популярные сценарии подготовки профилей для финансовой блокировки описаны в статье [Быстрый старт: Тарифный план и Captive Portal \(доступ к СЗР\)](#).

Утилита `fdpi_ctrl` является высокоскоростным API для управления DPI, пример: задание тарифного плана (настроек полисинга) сразу для 30 тысяч абонентов занимает меньше секунды времени:

```
time fdpi_ctrl load --policing rate_10M.cfg --file subscribers.lst
Result processing file 'subscribers.lst' : 30000/30000/0/0/0
real 0m0.344s
user 0m0.009s
sys 0m0.144s
```

Удаленный запуск команд через SSH

Для удаленного запуска команд на сервере DPI через SSH без ввода пароля рекомендуем использовать аутентификацию пользователей по публичным ключам.

Для этого на сервере управления:

1. создаем пару из публичного и закрытого ключей

```
ssh-keygen -t rsa
```

В диалоге выбираем значения по умолчанию. Секретную фразу для простоты дальнейшего использования оставляем пустой¹⁾

2. копируем публичный ключ на сервер DPI

```
ssh-copy-id dpi_user@dpi_host  
или ручками  
cat ~/.ssh/id_rsa.pub | ssh dpi_user@dpi_host "mkdir -p ~/.ssh && cat  
>> ~/.ssh/authorized_keys"
```

На сервере DPI проверяем и исправляем права на файл `authorized_keys`

```
chmod 700 ~dpi_user/.ssh/  
chmod 600 ~dpi_user/.ssh/authorized_keys  
restorecon -Rv ~dpi_user/.ssh/
```

Проверяем работоспособность удаленного запуска `fdpi_ctrl` с сервера управления

```
ssh dpi_user@dpi_host "fdpi_ctrl load --service 6 --login test"
```

Если запуск не работает, попробуйте найти подсказки в логе `/var/log/secure` на DPI сервере и включив на ssh диагностический режим: `ssh -v ...`

Удаленный запуск утилиты `fdpi_ctrl`

Для передачи команд на DPI используется TCP соединение через порт управления, поэтому необходимо разрешить в `firewall` внешний доступ по порту управления. Для того, чтобы DPI платформа принимала управляющие команды необходимо задать в конфигурационном файле `/etc/dpi/fastdpi.conf`: Номер прослушиваемого порта:

```
ctrl_port=29000
```

Имя сетевого интерфейса, по умолчанию DPI настроен на взаимодействие с через `lo`-интерфейс:

```
ctrl_dev=eth0
```

Для удаленного запуска утилиты `fdpi_ctrl` нужно произвести следующие действия:

1. в настроечном файле `dpi /etc/dpi/fastdpi.conf` включить прослушивание сетевого интерфейса управления, доступного извне

```
ctrl_dev=eth0
```

2. в настройках `firewall /etc/sysconfig/iptables` открыть доступ на порт, указанный в настройке `ctrl_port` и ограничить к хосту DPI доступ только с управляющего сервера

```
-A INPUT -m state --state NEW -m tcp -s 192.168.0.2 -p tcp --dport 29000 -j ACCEPT
```

3. скопировать утилиту `fdpi_ctrl` на управляющий сервер и запускать ее с аргументом `-r host:port`

```
fdpi_ctrl load --service 6 --login test -r 192.168.0.1:29000
```

ⓘ При обновлениях версии DPI нужно не забывать обновлять `fdpi_ctrl` на управляющем сервере

1)

либо используем возможности `ssh-agent` для хранения паролей